TELKOMNIKA, Vol 16, No 1: February 2018, pp. 323~333
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i1.6632

Comparison of Secret Splitting, Secret Sharing and Recursive Threshold Visual Cryptography for Security of Handwritten Images

Sugianto[1], Suharjito[2*], Nico Surantha[3]
[1]Information Technology Study Program, Information Management and Computer College, Institute of Business Development Indonesia, Medan 20114, Indonesia
[2,3]Computer Science Department, BINUS Graduate Program - Master in Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
*Corresponding author, e-mail: sugianto_shii@yahoo.co.id[1], suharjito@binus.edu [2]

Abstract

The secret sharing is a method to protect confidentiality and integrity of the secret messages by distributing the message shares into several recipients. The secret message could not be revealed unless the recipients exchange and collect shares to reconstruct the actual message. Even though the attacker obtain shares shadow during the share exchange, it would be impossible for the attacker to understand the correct share. There are few algorithms have been developed for secret sharing, e.g. secret splitting, Asmuth-Bloom secret sharing protocol, visual cryptography, etc. There is an unanswered question in this research about which method provides best level of security and efficiency in securing message. In this paper, we evaluate the performance of three methods, i.e. secret splitting, secret sharing, and recursive threshold visual cryptography for handwritten image security in terms of execution time and mean squared error (MSE) simulation. Simulation results show the secret splitting algorithm produces the shortest time of execution. On the other hand, the MSE simulation result that the three methods can reconstruct the original image very well.

Keywords: *secret sharing, splitting, visual cryptography*

1. Introduction

There is a classic problem when a group of people own a strictly confidential data. The confidential information could not be revealed by a single one of this group. Bruce Schneier provides an example of situation in his book Applied Cryptography. When there is a rocket launch that could not be activated by only one general, but it needs to be activated by several generals [1]. In this paper, security method for a handwritten image is discussed. The definition of handwritten image in this paper is a black and white image (binary/monochrome image) that is generated from the scan of hand-written document or image of document with text. The handwritten image may contain any confidential information or even secret military information acquired by a secret government agent. This image must be split into some fractions and stored independently. Every part of this image also needs to be encrypted to improve the security of the message. If the non-authorized party somehow can obtain the fraction of the image and decrypt the fraction, then he will be able to reveal the content of that image fraction.

Visual cryptographic methods, e.g. secret sharing, secret splitting, and visual cryptography can be implemented to solve this problem [2]-[3]. The secret splitting and secret sharing protocols can be applied to transform a message into several cipher-text segments that can be distributed to n people [4]. In secret splitting protocols, n cipher-text are required to recover the original message. On the other hand, in the secret sharing protocol, only m cipher-text from a total of n cipher-text are needed to recover the original message. This scheme is recognized as (m, n) schemes where m≤n. There are many algorithms of secret sharing have been proposed in the cryptographic literature. Asmuth Bloom is one of the most well-known secret sharing protocol [5]. Prime number and random number are utilized by this algorithm to improve the security of the secret message. In addition, n rows of number are required by this algorithm to meet the requirement. The ciphertext formation using Asmuth-Bloom algorithm is

Received Jun 11, 2017; Revised January 5, 2018; Accepted January 15, 2018

not complicated. It is conducted by modulo sum operation. Meanwhile, the original message reformation is relatively complicated. It requires Chinese remainder theorem [6]. Conventional secret sharing scheme is very inefficient in information theory. A secret sharing scheme (k, n) expands a secret message with length of b bits into n number of shares with a minimum size of b bits. Since only k share pieces required to reform the original secret, each bit in share holds a maximum of [1/k] bit of a secret. In case of non-threshold scheme (k=n), the information stored on every bit of the share is [1/n] bit of a secret [7].

Visual cryptography is one of the result of secret sharing scheme development. The aim of this method is to split a digital secret image into a number of shares. These shares should be compiled and stacked together to reform the original digital image without requiring any calculations. However, the conventional method of visual cryptography also have drawback in terms of efficiency, i.e. the number of secret bits stored per bit share. In 2002, recursive secrecy methods was introduced by Kak. S. to be applied to digital image and text[8],. The idea of this method is to conceal a secret message by splitting the secret message into smaller secret segments. Every segment will be stored/embedded recursively, with the size of segment secrets will be double at each step. As a result, it can increase the amount of information that can be stored on each bit of a secret. However, this scheme is categorized as a non-threshold scheme where all shares should be collected to recover the original secret. In 2010, Kak S, and Abishek Parakh developed the idea of secret hiding recursively into 2 of 3 threshold scheme and applied it to a secret digital image [9]. However this scheme can only be applied to binary images where each pixel is considered a one bit per information, representing a black or white pixel [6] Based on explanation of previous work in second and third paragraph, there is a question about which method provides the best level of security for securing handwritten images while provides high level of efficiency as well.

In this paper, we evaluate the performance of the three most well known secret image based sharing methods, i.e. secret splitting, secret sharing, and visual cryptography in securing the handwritten image. The parameters to be tested in the analysis include the length of execution time of the distribution process and reconstruction, image size share obtained along with the level of resistance to changes in the content of the image method share. After this research, we expect to give recommendation to readers about the best secret image based sharing method for securing handwritten image in terms of level of security and efficiency. This paper itself is organized as follow. Section 2 discusses about the literature review of three evaluated methods. Section 3 discusses about research methodology that is used in this paper. Section 4 discusses about the simulation result and analysis of the result. Finally, we conclude the result of the research in section 5.

2. Literature Review

When someone wants to transmit message with another party, the person surely wants the message to be safely transmitted. The safety here mean that the message could not be read by any unauthorized party. This safety issue recognized as message confidentiality [10]. In this section, we summarize the three visual cryptography method that we evaluate in this paper.

2.1. Secret Splitting

Secret spiltting method splits secret message into several shares and distribute them to some people with the aim to keep the secret of the message[11]. In this case, messages can represent the secret key that serves as the only access to information which is a highly confidential and sensitive. Secret Splitting utilizing random numbers generated by the multispeed-inner-generator. Secret splitting algorithm process is defined as follows:

a. Determine how many parts of a message (x), (P) to be split up.
b. Produce as much random numbers (x-1).
c. Perform the operations (1):
   $K(x)=K(1) \rho K(2) \rho K(3) \rho \ldots \rho K(x-1) \rho P$ (1)
d. K K (1), (2) ... K (x) and P is the fraction of the message is deleted.
   If there are others who change one bit in any pieces, then the message (P) will not be reopened.
e. To open or stir up a message (P), perform the operation (2)
   $P=K(1) \rho K(2) \rho K(3) \rho \ldots \rho K(x)$ (2)

2.2. Secret Sharing

Similar to public key cryptographic algorithm, the key formation of secret sharing algorithm produces the private key and public key. These keys are used in the formation of shadow. The private key and the public in Secret Sharing algorithm Asmuth-Bloom can be [12] defined as follows:

a. The public key (public key) of all users, which is primes p.
   Primes p can be raised by using the Rabin-Miller algorithm. Another way is to input manually and perform testing using an algorithm of primes testing method of Rabin-Miller. Primes p must be greater than the ASCII Code of the message. Since the value of the ASCII Code 255 is the largest primes, the value of p must be greater than 255.
b. The private key (private key) of each user, which is a row of values $d_1 \ldots d_n$.
   Row value d can be specified manually or generated randomly by meeting some of the following requirements:
   a) Row values d in ascending order, $d_i < d_{i+1}$.
   b) Each value d_i relatively Prime to any value d_i etc.
   c) $d_1 * d_2 * \ldots * d_m < p * d_{n-m+2} * d_{n-m+3} * \ldots * d_n$

Moreover, the process of forming the key will also generate values of m and n where m is the number of shadow values required to form the message and the value of n is the number of the desired shadow. The formation process of these keys can be described in the form of a flowchart as shown in Figure 1. The shadow formation of secret sharing algorithm can be described in the form of flowchart as shown by Figure 2.

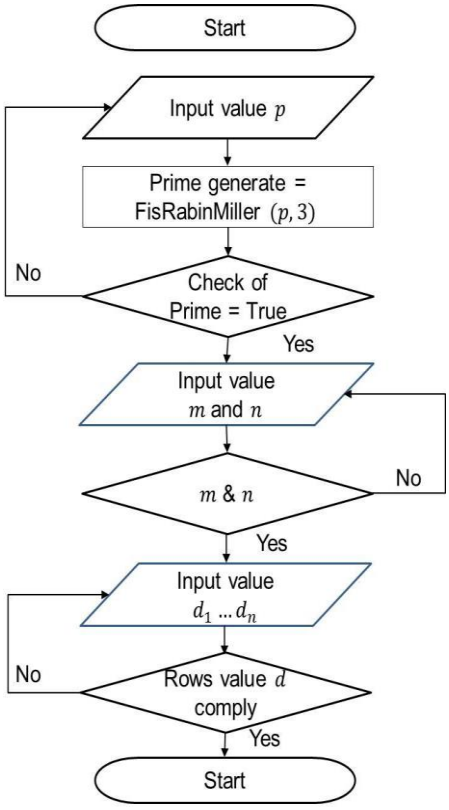


Figure 1. The key formation of asmuth-bloom secret sharing algorithm

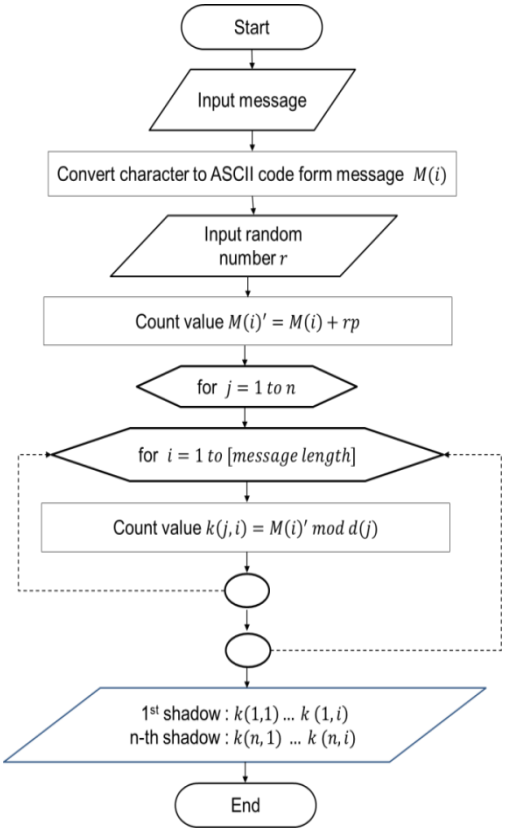


Figure 2. The shadow formation of asmuth-bloom secret sharing algorithm

The shadow formation of secret sharing algorithm uses the output of the key formation which is the private key and the public key of the user. The shadow formation of secret sharing

is performed by the author of the message. The result of this process is n shadows that are distributed to n person. Each person has a different value of the shadow.

The shadow merging process of secret sharing algorithm uses the output of the key formation which is the private key and the public key of the user. It also uses m shadow. The shadow merging process of secret sharing algorithm is performed by m people who want to reconstruct the original message. The result of this process is the original message that was concealed by the message's producer. The shadow merging process using Chinese Remainder Theorem is aimed to look for the solution of the linear congruent system formed from the combined m shadow and m values d_i [13]. The shadow merging process of Asmuth-Bloom secret sharing algorithm can be described in the form of flowcharts as Figure 3.

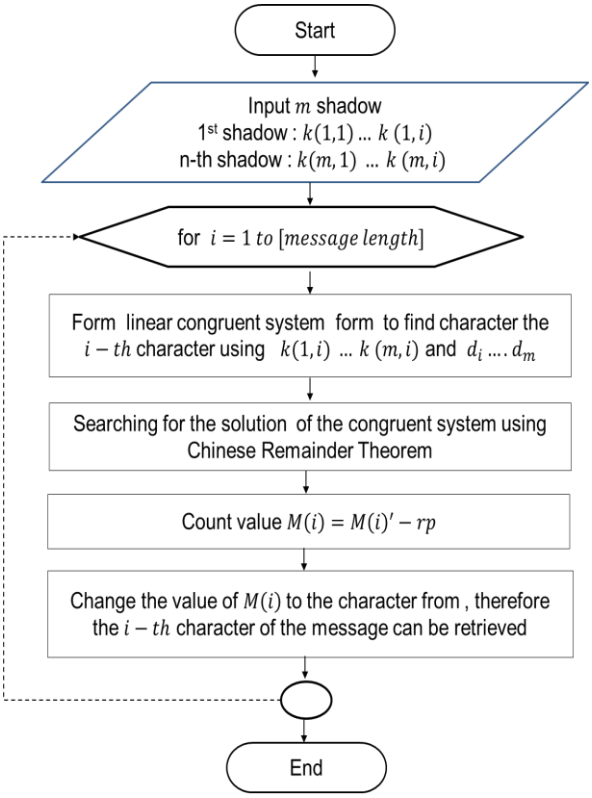


Figure 3. The shadow merging process of asmuth-bloom secret sharing algorithm

2.3. Threshold Visual Cryptography

The procedure of Recursive Threshold Visual Cryptography algorithm can be divided into two phases [14], i.e.:

a. The shadow formation phase: In this phase, a set of share files are generated. As for the procedure of work of this phase can be seen in Figure 4 [15]: The phase is started by entering the binary image and defining the number of k and n. Then, it check whether the image size is the rank of n. If yes, then it convert image to form a row of binary bits. If not, then it add white pixels until the height of image equals to the rank of n. Then the process is continued until n share is successfully generated.
b. Phase Merger Shadow, serves to reconstruct the original image by using a set of predetermined share. The working procedure of this phase can be seen in Figure 5: It is started by entering k image and numbers of n. Then it checks whether value of k > n. If yes, then it will enter another value of k. If no, then it converts images to form a row of binary bits. Then the process continued until the original image is successfully reconstructed.

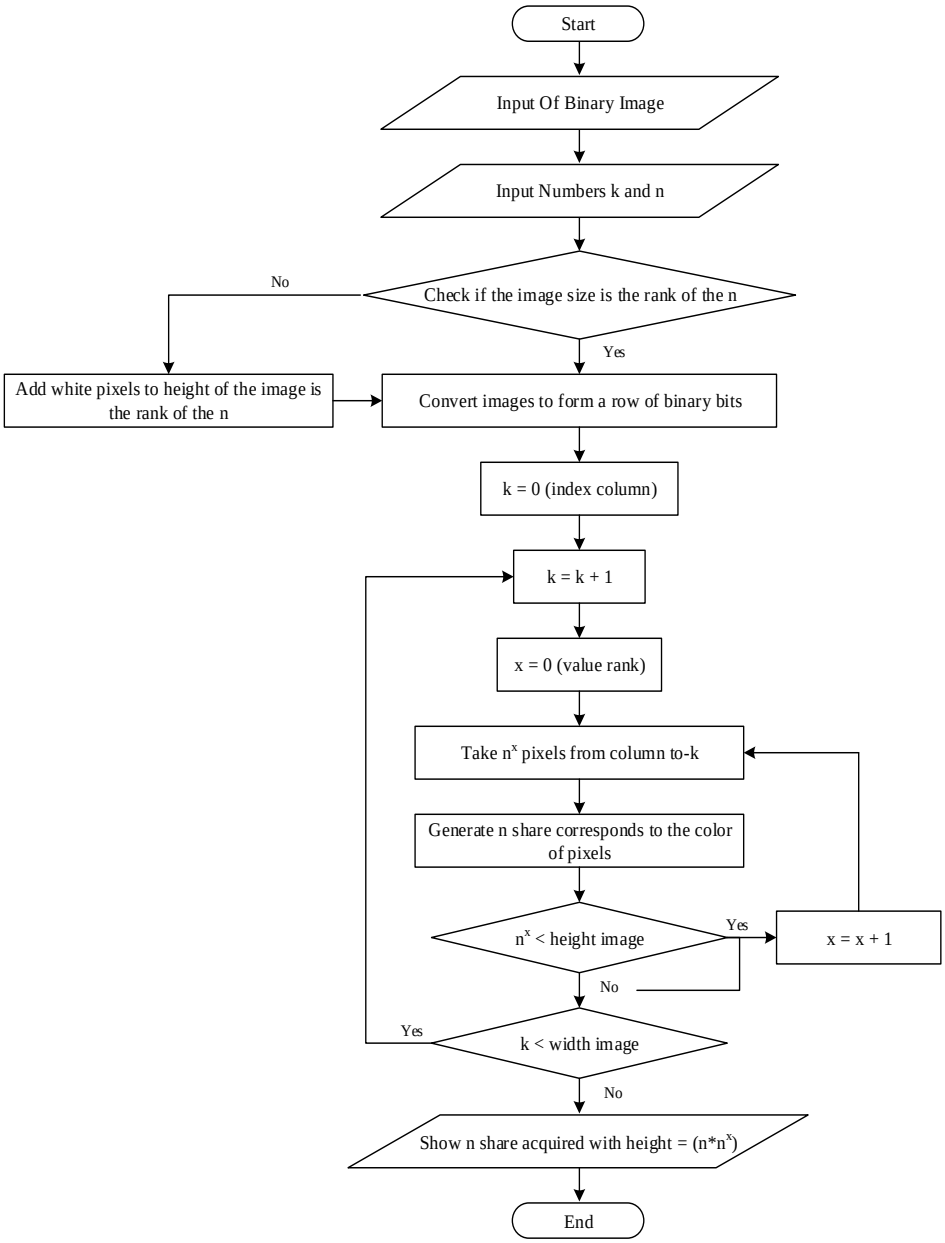


Figure 4. Flowchart of shadow formation phase

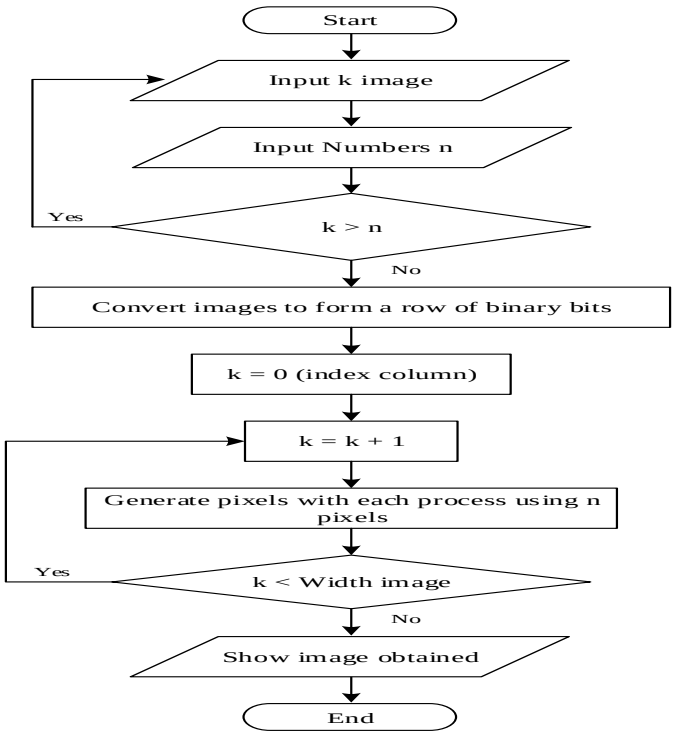


Figure 5. Flowchart of shadow merging phase

3. Research Method

In this research, we conduct a performance evaluation of the secret splitting, secret sharing and recursive threshold visual cryptography method in providing security to the handwritten image. The handwritten image can be either scanned images or images of handwritten text documents. The process of securing the handwritten image is started from identifying the problem to be solved. The problem is how to produce the share images and how to specify the method that is suitable for safeguarding the handwritten images. Then, the process is continued by selecting a suitalbe method which can be used. This process is performed by literature study, i.e. reading books and sources on the internet.Then, we continue to collect the data required in the system development process. After that, we create an application that can be used to test the performance of each method. Lastly, there will be an evaluation of the obtained test results. From the evaluation of the test results, the method that is suitable for securing the image of handwriting will be identified.

For the evaluation part, The performance of the three methods discussed is compared and evaluated using following method:

a. The length of time the execution of the manufacturing process and merger share (reconstruction) share. The number of digital images captured each of the 20 pieces of samples of [16]
b. The process of evaluation of the image of the reconstruction will use the formulation MSE. MSE can directly reflect the quality difference between the two digital images. MSE is used as a standard to calculate the quality of the original image and the image reconstruction results.

MSE between two images can be calculated using the following formula (3):

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}\left(P_1(i,j) - P_2(i,j)\right)^2 \quad (3)$$

Here, M, N is the width and height of the digital image, P1 (i, j) is the pixel value of the original digital image, and P2 (i, j) is the pixel value of the digital image reconstruction results [17].

4. Implementation and System Setup

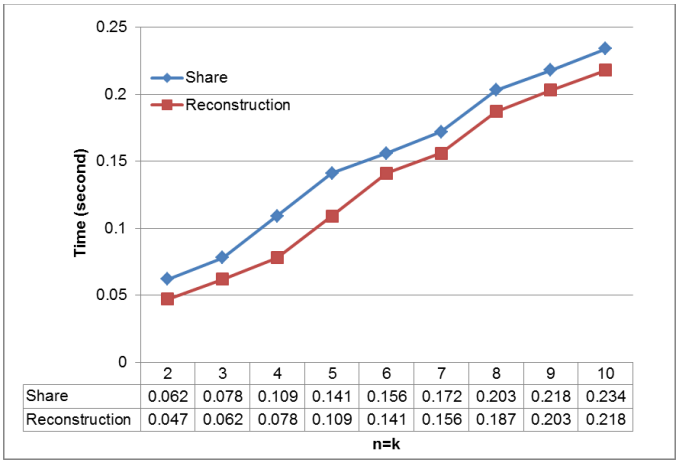
In order to run the experiment, we need the hardware and software as defined by Table 1. We perform the simulation using PC with processing capability pentium IV 2.6 GHz. We utilize Microsoft Visual Basic 6.0 to run the simulation.

Table 1. Hardware and Software Specification

Hardware Requirement		
No	Hardware Type	Specification
1	Processor	Pentium IV 2.6 GHz
2	RAM	256 MB
3	Storage	80 GB
4	Display	SVGA monitor resolution 1024 x 768
Software Requirement		
No	Software Type	Specification
1	Operating System	Windows 98/2000/XP
2	Tools	Microsoft Visual Basic 6.0

5. Result and Discussion

In this section, we discuss about simulation results. We evaluate the performance of three methods, i.e. secret splitting, secret sharing, and threshold visual cryptography in terms of execution time (share and reconstruction) and the mean squared error (MSE) of reconstructed image compared to the original secret image. We evaluate using n value=2-10. In this simulation, we do not perform testing to the share size produced by the three methods because secret splitting and sharing method do not generate additional pixels. Only the threshold visual cryptography method that producess share image with different pixel size from the original image.The size of image pixel produced by threshold visual cryptography method depends on the number of shared files generated (n value). Figure 6 shows the share and reconstruction time trend using secret splitting method for image size 100 ×100 pixel.

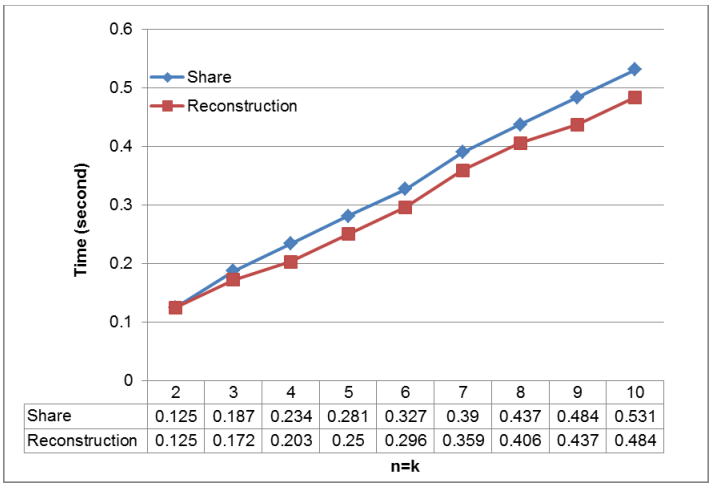


	2	3	4	5	6	7	8	9	10
Share	0.062	0.078	0.109	0.141	0.156	0.172	0.203	0.218	0.234
Reconstruction	0.047	0.062	0.078	0.109	0.141	0.156	0.187	0.203	0.218

Figure 6. Sharing and reconstruction time using secret splitting for image size 100x100 pixel

Figure 6 shows that the share and reconstruction time increases linearly as the increase of n value. From the value shown in the table, we can see that the value of share time when n=10 increases almost 4 times compared to share time when n=2. While the value of reconstruction time when n=10 increases almost 5 time compared to share time when n=2.

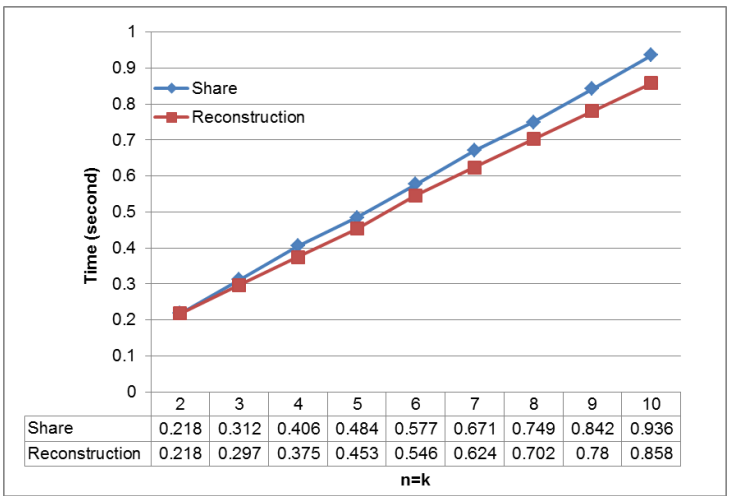
Figure 7 and Figure 8 show the share and reconstruction time using secret splitting method for image size 150 ×150 pixel and 200 ×200 pixel, respectively. If we compare the share time when n=10 for three image sizes, we can see that share time increase 2 times when image size increased to 150 ×150 pixel and the share time increases 4 times when image size increased to 200 ×200 pixel. The same trend also occurs for the reconstruction time. This result means that the share and reconstruction time increases linearly as the increase of image size.



	2	3	4	5	6	7	8	9	10
Share	0.125	0.187	0.234	0.281	0.327	0.39	0.437	0.484	0.531
Reconstruction	0.125	0.172	0.203	0.25	0.296	0.359	0.406	0.437	0.484

n=k

Figure 7. Sharing and reconstruction time using secret splitting for image size 150x150 pixel



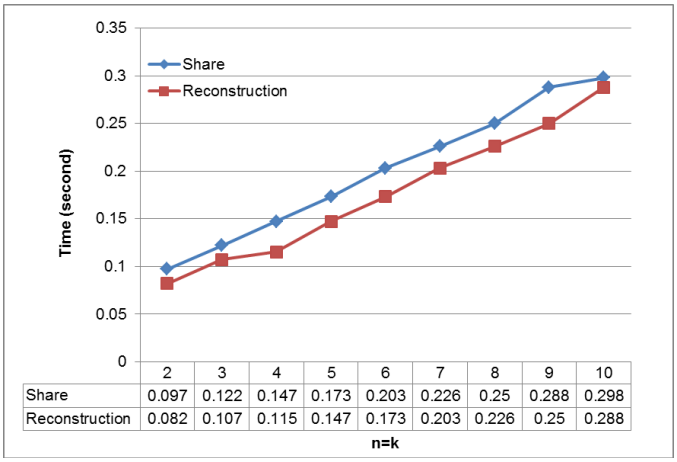
	2	3	4	5	6	7	8	9	10
Share	0.218	0.312	0.406	0.484	0.577	0.671	0.749	0.842	0.936
Reconstruction	0.218	0.297	0.375	0.453	0.546	0.624	0.702	0.78	0.858

n=k

Figure 8. Sharing and reconstruction time using secret splitting for image size 200x200 pixel

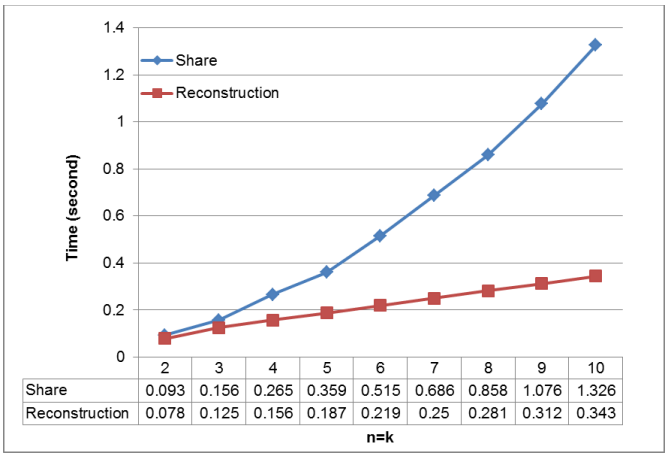
In the second testing, we compare the performance sharing and reconstruction time of secret splitting, secret sharing, and threshold visual cryptography. Figure 9 shows the share and reconstruction time using secret sharing method for image size 100 ×100 pixel. While Figure 10 shows the share and reconstruction time using threshold visual cryptography method for image size the same image size as the Figure 9. Figure 9 shows that using secret sharing method, the share and reconstruction time increase linearly as the increase of n value. While, interestingly, figure 10 shows that using the threshold visual cryptography method, the sharing time increase exponentially as the linear increase of n value. The exponential increase occurs due to the increase of share image size produced by threshold visual cryptography. When we compare the result of Figure 6, Figure 9, and Figure 10, we can also see that the secret splitting produces the

shortest share and reconstruction time among the three methods. It means the secret splitting is the most efficient algorithm among the three method for simulation parameter used in this paper. Therefore, we can conclude that the secret splitting is the most appropriate algorithm when applied practically.



	2	3	4	5	6	7	8	9	10
Share	0.097	0.122	0.147	0.173	0.203	0.226	0.25	0.288	0.298
Reconstruction	0.082	0.107	0.115	0.147	0.173	0.203	0.226	0.25	0.288

Figure 9. Sharing and reconstruction time using secret sharing for image size 100x100 pixel



	2	3	4	5	6	7	8	9	10
Share	0.093	0.156	0.265	0.359	0.515	0.686	0.858	1.076	1.326
Reconstruction	0.078	0.125	0.156	0.187	0.219	0.25	0.281	0.312	0.343

Figure 10. Sharing and reconstruction time using visual cryptography for image size 100x100 pixel

In the third testing, we evaluate the level of similarity between reconstructed image and the original image of the three methods. We perform mean squared error (MSE) calculation to evaluate the quality of the reconstructed image. We perform the simulation using n=2 -5 and image size are 100 ×100 pixel and 150 ×150 pixel. From the simulation results it shows that the MSE are zero for all scenario of simulation, which means the three methods shows excellent reconstruction for the simulation parameter used in this paper.

Based on the result of our simulation results and our literature study in this paper, we can evaluate the advantage and weakness of the three methods as follow: Secret splitting method execution time is the fastest among the three methods that makes this method is the most efficient when applied practically. It occurs because the secret splitting method contain a very simple algorithm. It only uses string and randomization algorithm operation XOR. However, the application of XOR operation makes the original image can be guessed easily if the tappers managed to obtain some file shares. Secret sharing method shows almost similar execution to the the secret splitting method. Secret sharing also perform better level of security due to the

involvement of Chinese Remainder method during the secret image reconstruction. The application of Chinese Remainder method is also very efficient when applied practically because the execution time is fairly quick. Furthermore the secret sharing method does not require all the file shares to reconstruct the orignal image, unlike the secret splitting. It means, the secret sharing is better in terms of reconstruction efficiency. Threshold visual cryptography method shows fairly quick execution time, eventhough it increases exponentially as the linear increase of n value. However, this method produces larger size of image files share compared to the original image. In addition, the threshold visual cryptography method only requires two pieces of the file share to reconstruct the original image. It means the attacker can reconstruct the image if they can collect only two images shares. In the future, it is interesting to perform the simulation and evaluation for bigger size of image and bigger n value to check the trend of MSE of the three methods.

6. Conclusion

In this paper, we have performed literature study and performance evaluation of security method for handwritten image. We have evaluated the performance of three most well known method, i.e. secret splitting, secret sharing, and threshold visual cryptography. In general the three methods contain a shadow making application that splits an image file into multiple file fragments shadow. The simulation results shows that secret splitting produces shortest execution time among the three methods which means it is the most efficient for practical situation. The MSE simulation shows that three methods shows excellent performance in image reconstruction. In the future, it is interesting to perform more simulation for various image size and number of share image (n value).

References

[1] Pakshwar R, Trivedi VK, Richhariya V. A Survey on Different Image Encryption and Decryption Techniques. *Int J Comput Sci Inf Technol.* 2013; 4(1): 113–6.
[2] Sharma A, Srivastava DK. A Comprehensive View on Encryption Techniques of Visual Cryptography. *Int J Recent Res Rev*. 2014; 7(2).
[3] Deng H, Song X. Chaos-Based Image Encryption Algorithm Using Decomposition. *Indones J Electr Eng Comput Sci.* 2014; 12(1):575–83.
[4] Yong-Jun G, Li-Zheng G, Ming-Hui Z. Improved Multi-secret Sharing Scheme Based on One-Way Function. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS).* 2014; 12(6): 4463-4467.
[5] Anbarasi LJ, Mala GSA, Prassana DRL. Visual Secret Sharing of Color Image Using Extended Asmuth Bloom Technique. *In: Computational Intelligence in Data Mining-Volume 3. Springer*; 2015: 555–62.
[6] Yan X, Lu Y, Liu L, Wan S, Ding W, Liu H. *Chinese Remainder Theorem-Based Secret Image Sharing for (k, n) Threshold.* In: International Conference on Cloud Computing and Security. 2017: 433–40.
[7] Farras O, Padró C, Xing C, Yang A. Natural generalizations of threshold secret sharing. *IEEE Trans Inf Theory.* 2014; 60(3): 652–64.
[8] Kumar S, Sharma RK. Recursive information hiding of secrets by random grids. *Cryptologia.* 2013; 37(2): 154–61.
[9] Parakh A, Kak S. Internet voting protocol based on improved implicit security. *Cryptologia*. 2010; 34(3): 258–68.
[10] Hwang SJ, Sung YH, Chi JF. Deniable authentication protocols with confidentiality and anonymous fair protections. *In: Advances in Intelligent Systems and Applications-Volume 2. Springer*; 2013: 41-51.
[11] Husain AK, Rahman AARA. A New Scheme for Pseudo Random Numbers Generator Based on Secret Splitting. *Int J Soft Comput Eng (IJSCE)* ISSN. 2015; 2231–307.
[12] Muhammad YI, Kaiiali M, Habbal A, Wazan AS, Sani Ilyasu A. A secure data outsourcing scheme based on Asmuth--Bloom secret sharing. *Enterp Inf Syst.* 2016; 10(9):1001–23.
[13] Harn L, Fuyou M, Chang C-C. Verifiable secret sharing based on the Chinese remainder theorem. *Secur Commun Networks.* 2014; 7(6): 950–7.
[14] Rathore AK, Jain A. A Review on Various Implemented Techniques for Visual Cryptography. *Int J Comput Appl.* 2016; 155(5).
[15] Yan X, Wang S, Niu X, Yang C-N. Generalized random grids-based threshold visual cryptography with meaningful shares. *Signal Processing.* 2015; 109: 317–33.

[16] Yann Lecun, Corrina Cortes CJCB. MNIST handwritten digit database, Yann LeCun, Corinna Cortes and Chris Burges [Internet]. [cited 2017 Dec 22]. Available from: http://yann.lecun.com/exdb/mnist/
[17] Candes EJ, Eldar YC, Strohmer T, Voroninski V. Phase retrieval via matrix completion. *SIAM Rev*. 2015; 57(2):225–51.